Amended pursuant to *Supreme Court Civil Rules* 6-1(1)(a). Original filed on October 30, 2024.

No. *Court File No.* ***VLC-S-S-247433***

Vancouver Registry

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN

KELLY STEGMAN

Plaintiff

AND

CENCORA, INC. and INNOMAR STRATEGIES INC.

Defendants

Brought under the *Class ~~Action~~ Proceedings Act,* [R.S.B.C. 1996], c. 50

<u>FIRST AMENDED</u> NOTICE OF CIVIL CLAIM

This action has been started by the plaintiff(s) for the relief set out in Part 2 below.

If you intend to respond to this action, you or your lawyer must

(a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim on the plaintiff.

If you intend to make a counterclaim, you or your lawyer must

(a) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim and counterclaim on the plaintiff and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

Time for response to civil claim

A response to civil claim must be filed and served on the plaintiff(s),

a) if you were served with the notice of civil claim anywhere in Canada, within 21 days after that service,

b) if you were served with the notice of civil claim anywhere in the United States of America, within 35 days after that service,

c) if you were served with the notice of civil claim anywhere else, within 49 days after that service, or

d) if the time for response to civil claim has been set by order of the court, within that time.

CLAIM OF THE PLAINTIFF

Part 1: STATEMENT OF FACTS

Parties and Overview

1. This action is brought because of the defendants' failure to properly secure and safeguard the plaintiff's and class members highly sensitive information ~~personal, financial and health information~~ from criminal hackers, including first/last name, address, date of birth, health diagnosis and condition, height, weight, phone number, email address, medical history, medications/prescriptions, medical record number, patient numbers, health insurance/subscriber number, signature, location of services, and lab results (Personal Health Information hereafter referred to as "PHI") together with financial records and social insurance numbers (Financial Information, hereafter referred to as "FI"). ~~medical prescriptions, financial records and SINs~~.

2. On or about February 21, 2024, Innomar Strategies Inc. ("Innomar") and Cencora Inc. ("Cencora"), a US based company, learned that it was the victim of a hack. On or about February 27, 2024, Cencora filed official notice of a hacking incident with the US Securities and Exchange Commission.

3. Starting on or about May 17, 2024, Cencora notified individuals whose information was compromised as a result of the hacking incident by informing them of the breach by letter mail. In the letters, Cencora said that the data from its systems included patient names, their postal address and date of birth, as well as information about their health diagnoses and

medications.

4. The plaintiff and class members continue to be at significant risk of identity theft and various other forms of personal, social, and financial harm.

The Plaintiff

5. Kelly Stegman ("Kelly") is a resident of Victoria, British Columbia. Kelly has a medical condition which required her to take certain medications supplied through Innomar Strategies, Cencora's Canadian affiliate.

6. On May 31, 2024, she received a letter from Cencora/Innomar ~~Strategies~~ informing her that "on February 21, 2024, Cencora learned that data from its information systems had been obtained by an unauthorized third party, some of which could contain personal information… On April 10, 2024, we confirmed that some of your personal information was affected by the incident."

7. On July 12, 2024, she received a second letter, which was largely the same as the first. Both letters informed her that "personal information, including your personal health information was affected, including potentially your first name, last name, address, date of birth, height, weight, telephone number, email address, dates and location of service, health diagnosis/condition, medications/prescriptions, medical record number, patient numbers, health insurances/subscriber number, signature, lab results, and medical history."

8. Both letters offered free ~~Credit Monitoring~~ credit monitoring services with TransUnion Canada for two years.

The Defendants

Cencora, Inc.

9. Cencora~~, Inc. ("Cencora")~~ is an international pharmaceutical solutions organization incorporated in Delaware with its principal place of business located at 1 West First Ave, Conshohocken, Pennsylvania, 19428.

10. Cencora provides medical products and services to patients and healthcare providers. The company was founded in 2001 and operates in more than 1,300 locations in 50 countries and ships more than 6.7 million products daily.

Innomar Strategies Inc

11. Innomar ~~Strategies Inc. ("Innomar")~~ is the Canadian subsidiary of Cencora and is a firm managing patient support programs. Innomar sometimes uses the name or trademark "Cencora Innomar Strategies", as pictured here from their website:

12. Innomar's services, as listed on their website, include pharmaceutical distribution and wholesale, pharmaceutical technology products and services, specialty business services that are focused on various pharmaceutical and pharmacy supply specialties such as specialty programs, clinic & nursing services, specialty pharmacy, specialty distribution & 3PL, strategic consulting, market access and reimbursement.

13. Innomar operates privately-owned facilities across Canada. There are nine InnomarClinics™ and one InnomarPharmacy™ in British Columbia. There are nine InnomarClinics™ and one InnomarPharmacy™ in Alberta. There are four InnomarClinics™ and one InnomarPharmacy™ in Saskatchewan. 7,293 individuals have been treated in InnomarClinics in Saskatchewan. There are ten InnomarClinics™ and three InnomarPharmacies™ in Ontario. There are three InnomarClinics™ and one InnomarPharmacy™ in Manitoba. There are ten InnomarClinics™ and two InnomarPharmacies™ in Quebec. There is one InnomarClinic™ in Newfoundland. The clinics provide services including lab testing and blood work, whereas the pharmacy provides personalized care.

14. The breach affected the PHI and FI of approximately 100,000 Canadians.

CLASS DEFINITION

15. The proposed class action is brought on behalf of all Canadian residents who were notified by Innomar ~~Strategies~~ that their information may have been compromised in the data breach.

FACTS

Cencora's Relationship to Class Members

16. Innomar positions itself as a 'middle-man' company which helps manufacturers of medicines (especially specialty medications which may require specialized treatment regimens) market and distribute those medications in Canada.

17. Innomar runs "patient support programs", an "InnomarPharmacy Network" and "InnomarClinics" where it collects PHI and/or FI ~~patient information~~ in order to provide medication or, in some cases, discounts on medication.

18. Innomar holds PHI and FI in connection with patient support programs (PSPs) that Innomar administers in partnership with various pharmaceutical companies. PSPs may include clinic and nursing and support (including infusion and injection administration/training), patient education and counselling, reimbursement navigation, and specialty pharmacy and logistics services. Innomar administers PSPs across Canada.

19. PSPs are administered by Innomar on behalf of its pharmaceutical partners, who ultimately own the data collected by Innomar. However, Innomar maintains custody of the PHI and FI collected in connection with PSPs. Although the plaintiff does not know all the details it appears that Innomar stored this information in a database that was connected in some way with the Cencora database and its affiliates' database. Given the location of Cencora and its' affiliates being in the United States, the plaintiff pleads that class member PHI and FI was also accessible in the United States.

20. Kelly's experience with Innomar is typical. Her medical condition required her to receive a specialized drug which was ultimately created by Roche Pharmaceuticals. To receive the drug, she attended at a specialty clinic where it was administered through IV infusion by a health care professional.

21. At the suggestion of her rheumatologist, Kelly enrolled in Innomar's JointEffort Program (Ontario). Her doctor, with her verbal consent, provided Innomar with an enrollment form and PHI ~~personal information~~ including her Public Health Number, Pharmacare patient number, and insurance data. They were provided with her mailing address, email address

and phone number.

22. Innomar asked Kelly (and received) consent to access her CRA notice of assessment and insurance information in order to determine whether she was entitled to a discount on the medication. This notice included her SIN.

23. As part of her ongoing treatment, Innomar was provided with Kelly's dosage of the medication, her other current medications, her height, ongoing weight measurements, and current health status, including whether she was suffering from a flu or cold from time to time.

24. As time went on, Kelly switched to a different medication, manufactured by Pfizer. However, Innomar was the medication and discount provider for the new medication as well. Innomar provided these services through a program called PfizerFlex. As a result, Kelly continued to provide her PHI and FI~~personal information~~ to Innomar.

25. The form Kelly's doctor filled out in order to allow her to access the Joint Effort's program included a consent (signed by her doctor on her behalf with her oral consent) to the provision of her PHI and FI ~~personal information~~ to Innomar. There is no reference in the form to how long the information would be kept or how it would be safeguarded. There is no reference to a privacy policy or statement. There was no disclosure that the information would be transferred to the United States and kept by Cencora.

26. Innomar's website, however, has a public facing privacy policy, available at https://www.innomar-strategies.com/privacy-policy (the "Privacy Policy"). The Privacy Policy divides information Innomar receives into "personal information that Innomar collects, uses, discloses and maintains for its own business purposes" which Innomar defines as "Personal Information" and "personal information that Innomar is required to collect, use and disclose for the purpose of services it is providing to a client" which Innomar defines as

"Client Personal Information." Innomar states that both categories include "personal health information."

27. Innomar's Privacy Policy states that "Innomar retains Personal Information only for as long as is necessary for the purpose for which it was collected. When Personal Information is no longer required, it will be destroyed or de-identified." The policy goes on to state that, "In the event that Personal Information is stolen, lost or accessed by unauthorized persons, Innomar will notify the individual to whom the information relates as required by law and, even where not legally compelled to give notice, *where we have reasonable grounds to believe that there exists a real risk of significant harm to the individual* to whom the information relates and there are steps that can be taken by the individual to mitigate that harm." (emphasis added).

28. With respect to "Client Personal Information", Innomar's Privacy Policy has a section entitled "Segregation, Return and Destruction of Client Personal Information". The section provides that "At a client's direction, Innomar will return or destroy the client's Client Personal Information, except as otherwise agreed to with the client or as required by law." There is no other provision for the retention or destruction of Client Personal Information.

29. Under "Security", which applies equally to both Personal Information and Client Personal Information in the Privacy Policy, Innomar states that:

2. Security

Innomar uses commercially reasonable physical, technological and administrative safeguards to safeguard Personal Information and Client Personal Information against theft, loss and unauthorized access, use (including copying and modification), disclosure and disposal while at rest and in transit.

The nature of the safeguards we use varies depending on the sensitivity, format, and the scope of the required distribution of the information, however they include:
a. by way of physical measures, safe storage of records, locked filing cabinets, and restricted access to offices;
b. by way of administrative/organizational measures, limiting access of Personnel on a "need- to-know" basis; and
c. by way of technological measures, the use of passwords for access to our electronic records systems, encryption and audits.

Personal Information and Client Personal Information held by Innomar is stored in one of two formats:
a. electronic databases or spreadsheets with restricted access located on servers and password protected; and/or
b. hard copy (paper) records that are kept in locked filing cabinets.

30. Innomar's Privacy Policy also provides that Innomar may transfer information out of the country. Although the details of Innomar and Cencora's relationship are not fully known by

the plaintiffs, it appears that class members' PHI and FI ~~class member information~~ was transferred to Cencora's database in the United States prior to the breach.

The Breach

31. On or about January 5, 2024, threat actors accessed the database of one of Cencora's affiliates. Once the threat actor was in the affiliate's database, based on the network segmentation arrangements at the time, it was able to use 'credentials' – a set of unique identifiers such as a username and password – from the affiliate's server to laterally move from the affiliate's systems into Innomar's systems. From there, the threat actors were able to exfiltrate PHI and FI from Innomar's systems.

32. Innomar, Cencora and Cencora's affiliate arranged their databases in such a way that by accessing one of the databases the malicious threat actors were able to access the other databases by using credentials that were improperly provided to one or more of Cencora's affiliates. Innomar failed to implement network segmentation rules that would have prevented this lateral access. The PHI and FI collected and maintained by Innomar was stored in the database in such a way that when threat actors gained access to Cencora's systems and/or one of Cencora's affiliates' systems, they were able to laterally access Innomar's systems.

33. Innomar has at least one other privacy policy, entitled a "Pharmacovigilance Privacy Policy", which contains much the same information as its Privacy Policy. That policy is available at https://www.innomar-strategies.com/pharmacovigilance-privacy-policy.

34. On February 21, 2024, Innomar and Cencora learned that data from Innomar's systems had been exfiltrated. After investigation, they found that the first evidence of "unauthorized interactive access" to their systems was on January 5, 2024, and the earliest evidence of exfiltration was from February 6, 2024. The threat actors had unimpeded access to Cencora's and Innomar's systems for over a month.

35. Cencora and Innomar collected class members' PHI and FI and retained said information on its servers and database and thus had custody over it.

36. On February 27, 2024, Cencora made a regulatory filing with the Securities and Exchange Commission in which it stated that it had learned on February 21 that data from IT systems "had been exfiltrated" at an unspecified earlier date. The regulatory filing did not specify the nature of the intrusion.

37. On April 10, 2024, Innomar and Cencora determined that Personal Health Information, such as names, addresses, dates of birth, height, weight, telephone number, email addresses, dates and location of services, health diagnosis/condition, medications/prescriptions, medical record numbers, patient numbers, health insurance/subscriber numbers, signature, lab results and medical history were a part of the PHI and FI that had been exfiltrated from its systems.

38. On or about May 17, 2024, roughly three months after Cencora learned that the class members' PHI and FI ~~Class's Private Information~~ was first accessed by cybercriminals and a month after its investigation was complete, Cencora finally began to notify patients that their data was affected. Kelly did not receive a letter telling her of the breach until May 31, 2024. This letter referenced her first medication. On June 12, 2024, she received a second letter telling her of the breach which appeared to be in relation to her participation in the PfizerFlex program.

39. The letters stated:

What Happened?

On February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which could contain personal information. Upon initial detection of the unauthorized activity, Cencora immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and outside lawyers. On April 10, 2024, we confirmed that some of your personal information was affected by the incident.

What Information Was Involved?

Based on our investigation, personal information including your personal health information was affected, including potentially your first name, last name, address, date of birth, height, weight, telephone number, email address, dates and location of service, health diagnosis/condition, medications/prescriptions, medical record number, patient numbers, health insurance/subscriber number, signature, lab results, and medical history. There is no evidence that any of this information has been or will be publicly disclosed, or that any information was or will be misused for fraudulent purposes as a result of this incident, but we are communicating this to you so that you can take the steps outlined below to protect yourself.

40. ~~The letter went on to offer two years of free credit monitoring through TransUnion.~~

41. ~~When asked by reporters, Cencora spokesperson Mike Iorfino stated that Cencora was~~

~~unwilling to say if the company had determined how many individuals were affected by the breach and how many individuals the company has notified to date. Cencora says on its website that it has served at least 18 million patients to date.~~

42. The company has so far declined to publicly describe what led to the data breach, such as whether the incident was caused by malicious hackers or a security lapse within the organization.

43. The breach impacted numerous Canadian patients enrolled in various patient support programs. As a result of the cyber security breach the plaintiff and class members' PHI and FI ~~personal information~~ has been intentionally accessed by cybercriminals on a computer/server without authorization.

44. The delayed communication regarding the breach and the potential for cross-referencing with other data breaches elevate the risk of financial harm and privacy violations to the plaintiff and other class members significantly.

45. There is a significant resale market for PHI and FI ~~medical information~~, because it can be used to supplement other records that could be used for identity theft.

46. The plaintiff and class members relied on the defendants to keep their PHI and FI ~~private information and their health information~~ confidential and securely maintained and to only make authorized uses of this information, which the defendants ultimately failed to do.

47. Thus, the plaintiff and class members have experienced fear and apprehension, anxiety, anger, risk, confusion and humiliation in relation to the unauthorized or unknown future use of their PHI and FI. ~~private information and their health information.~~

PART 2 – RELIEF SOUGHT

48. The plaintiff on her own behalf and on behalf of the class members, claims:

    a) an order pursuant to the *Class Proceedings Act [RSBC 1996] Chapter 333* (the "*CPA*"), certifying this action as a class proceeding and appointing the plaintiff as representative plaintiff of the class;

b) a declaration that the defendants breached *PIPEDA* and Provincial Personal Health Information Acts (as defined below);

c) a declaration that the defendants owed a duty of care to the plaintiff and the class in the handling, storage, and protection of their PHI and FI, ~~personal information,~~ as defined herein;

d) a declaration that the security breach was the result of the defendants breaching the standard of care required of them;

e) a declaration that one or both defendants breached their contracts with the plaintiff and the class and breached contracts to which the plaintiff and the class were third party beneficiaries, which resulted in the security breach;

f) a declaration that one or both defendants violated the privacy of the plaintiff and the class;

~~g) a declaration that the defendants breached the Consumer Protection Act, 2002, SO 2002, c 30, Sch. A; the Business Practices and Consumer Protection Act, SBC 2004, c 2; the Consumer Protection Act, RSA 2000, c. C-26.3, the Consumer Protection and Business Practices Act, SS 2013, c C-30.2; the Consumer Protection Act, CQLR c P-40.1; the Consumer Protection and Business Practices Act, SNL 2009, c C-31.1; Consumer Product Warranty and Liability Act, S.N.B. 1978, c. C-18.1; Sale of Goods Act, R.S.N.B. 2016, c. 110; Business Practices Act, R.S.P.E.I. 1988, c. B-7; and the Consumer Protection Act, R.S.P.E.I. 1988, c. C-19 (the "applicable consumer protection legislation");~~

~~h) Leave to dispense with notice to the defendants under section 18 of the Ontario *Consumer Protection Act* and any equivalent provisions in the applicable consumer protection legislation;~~

~~i) a declaration that the defendants breached the *Competition Act*, R.S.C. 1985, c. C-34 s. 52 and 36;~~

j) a declaration that the defendants breached ss. 3.2, 3.5, 5, 6, 10, 12, and 13 of the *Act Respecting the Protection of Personal Information in the Private Sector*, arts. 35, 36 and/or 37 of the Québec Civil Code and that, as a result, the class members resident in

Québec are entitled to moral and material damages pursuant to arts. 1457 and 1463-64 of the CCQ;

k) a declaration that class members resident in Québec are entitled to punitive damages pursuant to Article 49 of the Québec Charter of Human Rights and Freedoms;

l) general and special damages;

m) nominal damages for breach of contract;

n) an order directing an aggregate assessment of damages;

o) punitive damages

p) an order directing a reference or giving such other directions as may be necessary to determine any issues not determined at the trial of the common issues;

q) pre-judgment and post-judgment interest;

r) the costs of administering the plan of distribution of the recovery in this action; and

s) such further and other relief as this Honourable Court deems just.

PART 3 – LEGAL BASIS - CAUSES OF ACTION

49. Every class member has the right to informational privacy, being the right to control the use and disclosure of their PHI and FI and a reasonable expectation of privacy over said information. The privacy interest at issue was class members' right to expect Innomar to reasonably protect their PHI and FI from unauthorized access and disclosure.

Privacy Law / Regulatory Privacy Violations

50. As an organization which collected personal information across Canada, Innomar is subject to *PIPEDA*. The requirements of *PIPEDA* apply even when information collected in Canada is transferred outside of the country, as happened here. *PIPEDA* is mandatory, quasi-constitutional legislation. It requires, *inter alia*. the following:

    a) Innomar to be responsible and accountable for the PHI and FI ~~personal information~~ provided by its customers and to implement policies and practices to give effect

to the principles concerning the protection of the data (section 4.1 of Schedule I);

b) Innomar to seek and obtain the knowledge and consent of the class members for any collection, use or disclosure of the data including ongoing retention (section 4.3 Schedule I);

c) Innomar to confirm that class members' consent was "meaningful," requiring that "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed" (section 4.3.2 of Schedule I);

d) Innomar would protect the Class Members' User Account Data by adequate security safeguards that would prevent unauthorized access, disclosure, copying or use (section 4.7 of Schedule 1).

51. ~~At the direction of Cencora, Innomar transferred class member personal information to the Cencora servers in the US where it was hacked. The purpose of this transfer is unknown to the plaintiffs. To the extent that the purpose of the transfer was for the retention and safeguarding of the personal information, the plaintiff pleads that Cencora was an agent of Innomar in this transfer, and that both defendants owed duties to the class under PIPEDA.~~

52. ~~To the extent that the transfer was for any other purpose, the plaintiff pleads that Innomar failed to obtain any consent, much less meaningful consent, from class members when it transferred their sensitive personal and medical information to another company located outside Canada in the US. Instead, Innomar unilaterally transferred the information to Cencora's servers for some unknown purpose, where ultimately the information was exfiltrated by a hacker.~~

53. ~~In collecting and storing class members information in the US on its servers Cencora failed to notify class members it was in possession of their information, failed to obtain consent, much less meaningful consent, and failed comply with PIPEDA as set out in paragraph 41 of this claim.~~

54. The plaintiff pleads that Innomar collected and stored PHI and FI on its servers at an unknown location for an indefinite period of time. Innomar, Cencora and Cencora's affiliates intentionally arranged their information networks in such a way that a threat actor gaining access to Cencora's affiliate's database was then able to gain 'credentials' which allowed

them to gain lateral access to Innomar's network.

55. Contrary to PIPEDA, Innomar failed to obtain consent, much less meaningful consent as defined in PIPEDA, to:

a) The indefinite retention of class members' PHI and FI; and

b) the transfer of class members' PHI and FI to unsecured servers.

56. Contrary to PIPEDA, Innomar also failed to properly secure class members' PHI and FI.

57. The collection of personal health information in Canada is also governed by a series of provincial statutes;

a) Personal Health Information Protection Act, 2004, S.O. 2004, c 3, Sch A;

b) Health Information Protection Act, S.S. 1999, c H0.021;

c) Health Information Act, R.S.A. 2000, c H-5;

d) Personal Information Protection Act, S.B.C. 2003, c 63;

e) The Personal Health Information Act, CCSM c P33.5;

f) Personal Health Information Act, S.N.L. 2008, c P-7.01;

g) Health Information Privacy and Management Act, SY 2013, c 16;

h) Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05;

i) Act respecting the sharing of certain health information, CQLR c P9.0001;

j) Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q., c. P-39.1

k) Personal Health Information Act, SNS 2010, c 41;

l) Health Information Act, RSPEI 1988, c H-1.41;

m) Health Information Act, SNWT 2014, c 2.

58. These statutes are collectively referred to as the "Provincial Personal Health Information Acts".

59. The information collected by Innomar ~~and transmitted to Cencora~~ was "personal information" as defined in section 1 of the *Personal Information Protection Act* [SBC 2003] c. 63 ("PIPA BC") and the equivalent sections of the other Provincial Personal Health Information Acts.

60. Innomar and Cencora are "organizations" as defined in section 1 of PIPA BC and the equivalent sections of the other Provincial Personal Health Information Acts.

61. As the organization that collected and maintained PHI and FI ~~personal health information~~ from class members, Innomar had a duty to protect such ~~personal~~ information in its custody and under its control. ~~The plaintiff pleads that, to the extent that the transfer of personal information was done in order to retain and safeguard the information, Cencora was acting as the agent of Innomar for the purposes of protecting and safeguarding the information in Innomar's custody and control. Such transfer was a "use" of the information. As a result, both Innomar and Cencora owed duties under the Provincial Personal Health Information Acts (and PIPEDA) to protect and safeguard the information under their custody and control.~~

62. ~~In the alternative, to the extent that Cencora was not acting as an agent of Innomar at the time of the transfer, the transfer was an unauthorized disclosure of personal information contrary to the Provincial Personal Health Information Acts.~~

63. Pursuant to the Provincial Health Information Acts, Innomar was responsible for safeguarding class members' PHI and FI and preventing unauthorized access. PIPA BC, part 9, s. 34 requires an organization to "protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks." The other Provincial Personal Health Information Acts contain similar requirements.

64. Under PIPA BC, part 9, s. 35, Innomar was also responsible to destroy any documents containing personal information as soon as it was reasonable to assume that "the purpose for which that personal information was collected is no longer being served by retention of the personal information" and "retention is no longer necessary for legal or business purposes." The other Provincial Personal Health Information Acts contain similar

requirements.

65. Innomar and Cencora knew or ought to have known their network arrangement made it possible for threat actors who obtained credentials from Cencora's affiliates systems to laterally access Innomar's system. The storage and retention of the information by Innomar on the unsecured system was a "use" of the information.

66. By intentionally or recklessly failing to implement sufficient encryption and security, or proper network segmentation, the defendants breached PIPEDA and section 34 of PIPA BC which requires that an organization must protect personal information, such as PHI and FI, in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks and the equivalent sections of the other Provincial Personal Health Information Acts.

67. Innomar and Cencora breached ~~PIPEDA~~ section 35 of PIPA BC and principle 4.5 of PIPEDA by intentionally or recklessly failing to destroy class members' personal information, such as PHI and FI, when it was no longer needed, as required by those ~~that~~ sections and the equivalent sections of the other Provincial Personal Health Information Acts.

68. The standards set out under PIPEDA and the Provincial Personal Health Information Acts, and the breaches of those standards set out above, inform the statutory privacy tort cause of actions set out below.

Breach of Contract

69. Class members signed (or otherwise authorized) "consents" for their health practitioners to share their PHI and FI ~~medical and personal information~~ with Innomar for the limited purpose of ~~Innomar~~ "providing or coordinating " medical services and drugs. (the "~~c~~Contract").

70. It was an implied term of the ~~c~~Contract that Innomar in its capacity as data custodian would comply with PIPEDA and equivalent provincial legislation including to keep all class member information confidential, properly secured and would not retain it longer than was required to provide medical services ~~would keep all class member information confidential and comply with all mandatory privacy legislation. The contract was a unilateral contract which class members were required to agree to in order to receive the medication and medical~~

~~services they needed.~~.

71. ~~The contract contained no reference to Innomar's privacy policies, which are therefore not incorporated by reference. The contract is silent as to how long Innomar can retain personal information, how Innomar will protect it and whether the personal information can be transferred to others such as Cencora or outside Canada.~~

72. ~~Instead, in exchange for the client personal information, in the "consents" Innomar promised it would "use or disclose" class members' personal information "only for the purpose of providing and coordinating [the relevant medical] services… or as authorized or required by law." The Contracts did not provide that Innomar could send the information to its parent company, Cencora, nor did they refer to any reason for doing so.~~

73. Innomar breached the express term of the Contract, its promise to class members to use their PHI and FI ~~personal information~~ "only for the purposes of providing or coordinating" medical services by ~~sending the personal information to its parent company, Cencora, in the United States. The information was sent for Innomar and Cencora's own business purposes and not for the purpose of providing and coordinating medical treatment.~~ using the information for other purposes including storing the data on its servers in the United States.

74. Innomar breached the implied term of the Contract by failing to comply with PIPEDA and equivalent provincial legislation to keep the PHI and FI confidential from Cencora and its affiliates and secure. It breached its safeguarding obligations in its capacity as the data custodian by arranging its network systems in such a way that threat actors could obtain 'credentials' and laterally move from Cencora's affiliate's database into Innomar's database. ~~sending the personal information to its parent company, Cencora, in the United States. The information was sent for Innomar and Cencora's own business purposes and not for the purpose of providing and coordinating medical treatment.~~

75. ~~In the alternative, and to the extent that Cencora acted as an agent for Innomar in accepting the transfer of personal information, the plaintiffs plead that it was an implied term of the contract that Innomar and its agents would properly safeguard class members' personal information to ensure that it was "use[d] or disclose[d]" only for "the purpose of providing and coordinating [the relevant medical] services." The plaintiffs plead that Innomar and Cencora breached the contracts by failing to adequately protect class members' personal~~

~~information.~~

76. ~~The plaintiffs plead that Innomar's privacy policies did not form part of the Contracts, because they were not referenced in them. The privacy policies were not drawn to class members attention, and Innomar did not seek to condition class members' provision of their personal information to the privacy policies.~~

77. Innomar's lax cyber security and failure to implement proper network segmentation at the time breached the implied term of the Contract that Innomar would keep class members' PHI and FI confidential and properly secured.

78. Innomar also breached the implied term of the Contract that it would not retain class member PHI and FI after its services were no longer required.

79. In the alternative, the ~~plaintiffs plead~~ plaintiff pleads that if the privacy policies formed part of the Contract~~s~~, the defendants breached the privacy policies by:

    a) failing to provide the level of security set out in section 2 of the Policy;

    b) ~~transferring and~~ storing client PHI and FI ~~personal information~~ in the United States (a use of the personal information) without disclosing an intent to do so or obtaining consent; and

    c) failing to delete, deidentify or destroy Personal Information and Client Personal Information (as defined in the privacy policies) when it was no longer required.

80. As a result of these breaches of contract, the plaintiff and class members suffered damages as further particularized below.

Negligence (Innomar)

81. Class members contracted directly with Innomar to receive medical services (or access to discounted medical services). Through this process, class members provided PHI and FI ~~personal information~~ to Innomar, who collected and maintained class members' PHI and FI in order to provide services. The information was also stored on Cencora's database. ~~then transferred it to Cencora.~~

82. ~~The plaintiff pleads that Innomar remained responsible for the protection of the PHI and FI~~

~~personal information even after it was it was transferred to Cencora pursuant to PIPEDA and the Provincial PHI Acts. In these circumstances,~~ The ~~the plaintiff pleads that Innomar is liable for any negligent acts of Cencora as hereinafter described and owed a duty of care to the class members as hereinafter described.~~

83. Innomar owed a duty of care to the class members in their collection, use and retention of the PHI and FI ~~personal information~~, to keep the PHI and FI ~~personal information~~ confidential and secure, and to ensure that when it was stored on Cencora's and/or Innomar's systems ~~transferred to Cencora~~ it would not be lost, disseminated or disclosed to unauthorized persons and to delete and destroy PHI and FI ~~personal information~~ of class members when those class members no longer needed access to Innomar's services. Thus, the class members had a reasonable expectation that no one would access their PHI and FI absent express consent and that recipients of their PHI and FI would protect their privacy interests.

84. Specifically, this defendant owed a duty of care to the class members to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack, to ensure that any entity which it entrusted with PHI and FI ~~personal information~~ did the same, and to take appropriate steps to limit the exposure of the class members' PHI and FI ~~personal information~~ even in case of a successful cyberattack.

85. There was a sufficient degree of proximity between the class members and Innomar to establish a duty of care because:

    a) Their close and direct relationship with each Class Member arising out of the Contract~~s~~ and their collection, creation, use, storage, and transmission of class members PHI and FI ~~personal information~~ in connection with the provision of medical services to class members;

    b) Innomar's acknowledgements and commitments regarding the need to protect the personal information, such as PHI and FI, set out in its privacy policies;

    c) it was reasonable for the plaintiff and other class members to expect that Innomar had implemented appropriate security safeguards against a cyberattack and to limit the exposure of their PHI and FI ~~personal information~~ in case of a cyberattack, especially where the defendants held themselves out to class members as having rigorous privacy standards to protect class members' privacy;

d) it was reasonably foreseeable to Innomar that, if a cyberattack resulted in the theft of the class members' PHI and FI ~~personal information~~, the class members would sustain damages, such that the defendant should have been mindful of the class members' privacy and on guard against a cyberattack;

e) it was reasonably foreseeable to Innomar that, if it failed to take appropriate security measures and to implement programs and policies designed to protect PHI and FI ~~personal information~~, or to ensure that parties that it contracted with did the same, there was a risk that the class members' privacy would be breached, because of the sensitivity of the types of data collected and stored, and the climate of increasing cyberattacks targeted toward institutions which collect sensitive and private information;

f) the class members were entirely vulnerable to Innomar, in terms of relying on Innomar to take appropriate security measures to protect their PHI and FI; ~~personal information~~; and

g) Innomar was required by sections 4.1, 4.5 and 4.7 of Schedule 1 to PIPEDA and equivalent provisions in the Provincial Personal Health Information Acts, to implement safeguards appropriate to the sensitivity of the information stored on their network. ~~;~~

86. The standard of care the defendants were required to meet with respect to the collection and storage of PHI and FI ~~personal information~~ was heightened given the highly sensitive nature of the information that they were entrusted with. The required standard is informed by, but not limited to, industry practice, the common law, and the privacy legislation outlined above at paragraphs ~~44 to 51~~ 57-67. The defendants were mandated by statute and common law to have in place effective, updated, state of the art cybersecurity to protect the sensitive information that they collected and stored.

87. The defendants did not meet the standard of care. Particulars of their breaches include, but are not limited to intentionally, willfully, recklessly and negligently:

a) failing to handle the collection, retention, security and disclosure of the class members' personal information, such as PHI and PI, in accordance with their obligations under the contract, PIPEDA, and the Provincial Personal Health

Information Acts;

b) allowing the PHI and FI ~~personal information~~ to be used and disclosed for purposes other than those for which it was collected, contrary to s. 4.5 of Schedule 1 to PIPEDA and the equivalent provisions of the Provincial Personal Health Information Acts;

c) failing to confirm that Cencora had proper risk assessment policies, penetration testing strategies or that it had sufficient basic security controls;

d) storing unencrypted, or weakly encrypted, PHI and FI ~~personal information~~ on ~~Cencora's~~ systems, potentially in the United States, which were not properly secured from each other, allowing threat actors to gain 'credentials' and lateral access to one system from another;

e) collecting and storing more ~~personal health information~~ PHI than was necessary;

f) failing to maintain adequate or any surveillance and systems checks over the systems;

g) failing to train employees to identify and respond appropriately to phishing and other common attacks; ~~and~~

h) failing to delete and destroy stored PHI and FI ~~Personal Information~~ after there was no longer a legitimate purpose for retaining it; and

i) failing to take any steps or all reasonable steps to remedy the alleged privacy breach in a timely and meaningful manner in particular, by not warning class members that their PHI and FI had been hacked for three months after the defendants first learned of the breach or offering sufficient free credit monitoring services such as monitoring by both Trans Union and Equifax and for at least ten years.

88. Innomar's ~~negligent~~ conduct caused the plaintiff and class members to suffer a violation of their right to informational privacy and reasonable expectation of privacy with attendant harm and damages, as particularized below. The plaintiff pleads that ~~these damages flow from~~ the privacy violation constitutes an injury to her person and/or property (and to the

persons and/or property of class members) in the form of an invasion of privacy. ~~and a violation of her and class members' privacy rights.~~

Negligence (Cencora)

89. At some point unknown to the plaintiff, Cencora contracted with Innomar to provide services to Innomar with respect to the retention and protection of class members' PHI and FI ~~personal information~~. Through this process, Cencora received and stored class members' PHI and FI ~~personal information~~.

90. Cencora owed a duty of care to the class members in their collection, use and retention of the PHI and FI ~~personal information~~, to keep the PHI and FI ~~personal information~~ confidential and secure, and to ensure that when it was ~~transferred to~~ stored on Cencora's systems it would not be lost, disseminated or disclosed to unauthorized persons and to delete and destroy PHI and FI ~~personal information~~ of class members when those class members no longer needed access to Cencora's services. Thus, the class members had a reasonable expectation of privacy that no one would access their PHI and FI absent express consent and that recipients of their PHI and FI would protect their privacy interests.

91. Specifically, this defendant owed a duty of care to the class members to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack, to ensure that any entity which it entrusted with PHI and FI ~~personal information~~ did the same, and to take appropriate steps to limit the exposure of the class members' PHI and FI ~~personal information~~ even in case of a successful cyberattack.

92. There was a sufficient degree of proximity between the class members and Cencora to establish a duty of care because:

    a) it was reasonable for the plaintiff and other class members to expect that any company who received their personal information, such as PHI and FI, from Innomar for retention purposes, including Cencora, had implemented appropriate security safeguards against a cyberattack and to limit the exposure of their PHI and FI ~~personal information~~ in case of a cyberattack, especially where the defendant Innomar, with the consent and knowledge of Cencora, held itself out to class members as having rigorous privacy standards to protect applicants' and

customers' privacy and would ensure any third party with whom it shared personal information would maintain the same standard;

b) it was reasonably foreseeable to Cencora that, if a cyberattack resulted in the theft of the class members' PHI and FI ~~personal information~~, the class members would sustain damages, such that the defendant should have been mindful of the class members' privacy and on guard against a cyberattack;

c) it was reasonably foreseeable to Cencora that, if it failed to take appropriate security measures and to implement programs and policies designed to protect PHI and FI ~~personal information~~, or to ensure that parties that it contracted with did the same, there was a risk that the class members' privacy would be breached, because of the sensitivity of the types of data collected and stored, and the climate of increasing cyberattacks targeted toward institutions which collect sensitive and private information;

d) the class members were entirely vulnerable to Cencora, in terms of relying on Cencora to take appropriate security measures to protect their PHI and FI ~~personal information~~; and

e) As a recipient of the PHI and FI ~~personal information~~ of Canadians, Cencora was required by sections 4.1, 4.5 and 4.7 of Schedule 1 to PIPEDA and equivalent provisions in the Provincial Personal Health Information Acts, to implement safeguards appropriate to the sensitivity of the information stored on their network;

93. The standard of care the defendants were required to meet with respect to the collection and storage of PHI and FI ~~personal information~~ was heightened given the highly sensitive nature of the information that they were entrusted with. The required standard is informed by, but not limited to, industry practice, the common law, and the privacy legislation outlined above at paragraphs 57 to 67 ~~44 to 51~~. The defendants were mandated by statute and common law to have in place effective, updated, state of the art cybersecurity to protect the sensitive information that they collected and stored.

94. The defendants did not meet the standard of care. Particulars of their breaches include, but are not limited to intentionally, willfully, recklessly and negligently:

a) failing to handle the collection, retention, security and disclosure of the class members' personal information, such as PHI and FI, in accordance with their obligations under the contract, PIPEDA, and the Provincial Personal Health Information Acts;

b) allowing the PHI and FI ~~personal information~~ to be used and disclosed for purposes other than those for which it was collected, contrary to s. 4.5 of Schedule 1 to PIPEDA and the equivalent provisions of the Provincial Personal Health Information Acts;

c) failing to have proper risk assessment policies, penetration testing strategies or that it had sufficient basic security controls;

d) ~~it failed~~ failing to implement appropriate physical, organizational and technological safeguards to protect the PHI and FI ~~personal information~~ against loss, theft, unauthorized access, disclosure, copying, use, and/or modification, contrary to s. 4.7 of Schedule 1 to the PIPEDA;

e) ~~it failed~~ failing to use any, or appropriate, cybersecurity measures, programs and policies (including encryption) to safeguard the class members' PHI and FI ~~personal information~~, or ~~it used~~ using cybersecurity measures, programs and policies which were outdated, inadequate, and below the reasonable industry standards;

f) ~~it failed~~ failing to hire competent employees, ~~it failed~~ failing to properly supervise their employees, or ~~it failed~~ failing to provide proper training to its employees;

g) failing to maintain adequate or any surveillance and systems checks over the systems;

h) failing to train employees to identify and respond appropriately to phishing and other common attacks; ~~and~~

i) failing to delete and destroy stored PHI and FI ~~Personal Information~~ after there was no longer a legitimate purpose for retaining it~~.~~; and

j) failing to take any steps or all reasonable steps to remedy the alleged privacy breach in a timely and meaningful manner in particular, by not warning class members that their PHI and FI had been hacked for three months after the

defendants first learned of the breach or offering sufficient free credit monitoring services such as monitoring by both Trans Union and Equifax and for at least ten years.

95. Cencora's ~~negligent~~ conduct caused the plaintiff and class members to suffer a violation of their privacy rights with attendant harm and damages as particularized below.

Statutory Torts for Privacy Violations

96. ~~The defendants~~ Innomar substantially, unreasonably, willfully, and without claim of right violated the privacy of the plaintiff and other class members by willfully, intentionally and recklessly ~~permitting the unauthorized use of~~ setting up their database in such a way as to permit criminals to gain access to the plaintiff's and other class members' PHI and FI ~~personal information, health data, and data set out in the whole of this claim~~, in violation of the Privacy Policies and their contracts with class members.

97. It was a violation of class members' right to informational privacy and expectation of privacy for Innomar to set up their database in such a way that a threat actor would be able to laterally move into their database from Cencora's or Cencora's affiliate's system.

98. It was also a privacy violation for Cencora to willfully, intentionally or recklessly provide one or more of its affiliates with the credentials to gain access to class members' PHI and FI absent consent from the class members.

99. Innomar had an obligation to satisfy itself that when setting up their database, a threat actor would not be able to laterally move into their database from Cencora's or Cencora's affiliate's system.

100. Cencora also had an obligation to act to satisfy itself that its affiliates had appropriate security measures, policies and practices in place to prevent malicious actors from accessing the credentials. Its failure to act in circumstances when there was an obligation to do so constituted willful and intentional misconduct, recklessness, willful blindness and reckless indifference to the possible consequences of their actions.

101. The defendants' failures to comply with PIPEDA and the Provincial Personal Health Information Acts, as set out above inform the violations of the statutory torts.

102. With respect to the plaintiff and class members resident in British Columbia, Manitoba, Saskatchewan, and Newfoundland and Labrador, the plaintiff pleads and relies on the *Privacy Act,* RSBC 1996, c 373; *The Privacy Act,* CCSM c Pl 25; *The Privacy Act,* RSS 1978, c P- 24; and *The Privacy Act,* RSNL 1990, c P-22 (the "Statutory Torts"). In each of these jurisdictions, Cencora and Innomar willfully, intentionally ~~or~~ and recklessly violated class member privacy. In all four provinces the tort is actionable without proof of damage.

103. ~~With respect to class members resident in Québec, the plaintiff pleads that Cencora and Innomar violated Sections 5, 6, 10, 12, and 13 of the Act respecting the protection of personal information in the private sector, C. P-39.1 ("Private Sector Act");~~

104. The facts pleaded in support of the violations of privacy are set out above under the section "Privacy Law/Regulatory Privacy Violations".

105. As a result, class members suffered damages including general damages, compensatory damages, ~~and~~ moral damages, and pecuniary damages as further particularized below.

British Columbia

106. The plaintiffs plead on behalf of all class members who are domiciled or are residents of the Province of British Columbia, that the defendants violated section 1 of the *Privacy Act*, *RSBC 1996, c. 373,* as amended.

107. Cencora and Innomar ~~Strategies~~, without a claim of right intentionally, willfully and recklessly violated the privacy of the British Columbia class members when ~~its intentional and reckless acts~~ it allowed unauthorized third parties (cybercriminals) to access their PHI and FI ~~personal and health information~~ without the class members' consent.

108. Moreover, by making the PHI and FI available to its affiliates without any safeguards and with knowledge of its potential for misuse, Innomar in its capcity as the data custodian violated section 1(1) of the Privacy Act.

Manitoba

109. The plaintiff pleads on behalf of all class members who are domiciled or are

residents of the Province of Manitoba, that the defendants violated section 2 of the *Privacy Act, CCSM c. P125*, as amended.

110. Cencora and Innomar ~~Strategies~~, substantially, unreasonably, and without a claim of right violated the privacy of the Manitoba class members when it allowed unauthorized third parties (cybercriminals) to access their PHI and FI ~~personal and health information~~ without the class members' consent.

111. As a result of this breach the Manitoba class members are entitled to rely upon section 4 of the *Privacy Act, CCSM c. P125*, as amended.

112. Moreover, by making the PHI and FI available to its affiliates without any safeguards and with knowledge of its potential for misuse, Innomar in its capacity as the data custodian violated section 2 of the Privacy Act.

Saskatchewan

113. The plaintiff pleads on behalf of all class members who are domiciled or are residents of the Province of Saskatchewan, that the defendants violated section 2 of the *Privacy Act, RSS 1978, c P-24,* as amended 1996.

114. Cencora and Innomar ~~Strategies~~ without a claim of right intentionally, willfully and recklessly violated the privacy of the Saskatchewan class members when ~~its intentional and reckless acts~~ it allowed unauthorized third parties (cybercriminals) to access their PHI and FI ~~personal and health information~~ without the class members' consent.

115. Moreover, by making the PHI and FI available to its affiliates without any safeguards and with knowledge of its potential for misuse, Innomar in its capacity as the data custodian violated section 2 of the Privacy Act.

~~Québec~~

116. ~~The plaintiff pleads on behalf of all class members who are domiciled or are residents of the Province of Québec, that the defendants collected personal information from class members. The plaintiff further pleads that the transfer of information from Innomar to Cencora was a "collection of personal information" by Cencora which was done without consent and~~

~~was a use contrary to the purpose for which it was collected, contrary to ss. 6, 12, and 13 of the Private Sector Act.~~

117. ~~The plaintiff further pleads that Innomar and Cencora failed to take the security measures necessary to ensure the protection of the personal information collected, contrary to s. 10 of the Private Sector act.~~

Newfoundland and Labrador

118. The plaintiff pleads on behalf of all class members who are domiciled or are residents of the Province of Newfoundland and Labrador, that the defendants violated section 3 of the *Privacy Act, RSNL 1990, c P-22*, as amended.

119. Cencora and Innomar ~~Strategies~~ without a claim of right intentionally, willfully and recklessly violated the privacy of the Newfoundland and Labrador class members when ~~its intentional and reckless acts~~ it allowed unauthorized third parties (cybercriminals) to access their PHI and FI ~~personal and health information~~ without the class members' consent.

120. ~~The hacker also breached the statutory torts by willfully violating the privacy of class members by exfiltrating their sensitive personal and medical information.~~

121. Moreover, by making the PHI and FI available to its affiliates without any safeguards and with knowledge of its potential for misuse, Innomar in its capacity as the data custodian violated section 3 of the Privacy Act.

Breach of Québec Law ~~the Québec Civil Code ("CCQ")~~

122. With regard to the class members resident in Québec, the defendants breached articles 35, 36 and/or 37 of the CCQ by failing to maintain adequate cybersecurity to safeguard the class members' PHI and FI ~~personal and health information~~ from unauthorized access.

123. More particularly, the defendants breached articles 35, 36, and 37 of the CCQ because they allowed unauthorized access to the PHI and FI ~~personal and health information~~ of the class members resident in Québec without their consent and without the invasion being authorized by law.

124. The plaintiff pleads that Cencora and Innomar violated Sections 3.2, 3.5, 5, 6, 10, 12, and 13 of the *Act respecting the protection of personal information in the private sector*, C. P-39.1 ("Private Sector Act"), which informs the rights of Quebec residents under articles 35, 36, and 37 of the CCQ.

125. The plaintiff pleads on behalf of all class members who are domiciled or are residents of the Province of Québec, that the defendants collected PHI and FI ~~personal information~~ from class members. The plaintiff further pleads that the indefinite retention of PHI and FI was a "collection of personal information" by Innomar which was done without consent and was a use contrary to the purpose for which it was collected, contrary to ss. 3.2, 6, 12, and 13 of the Private Sector Act.

126. The plaintiff further pleads that Innomar and Cencora failed to take the security measures necessary to ensure the protection of the PHI and FI ~~personal information~~ collected, contrary to ss. 3.5 and 10 of the Private Sector Act.

127. The plaintiff pleads that the defendants' breaches of contract, as particularized at paragraphs 69-80 above, constituted a breach of section 1458 of the CCQ.

128. The plaintiff pleads that the defendants' negligence, as particularized at paragraphs 81-95 above, constituted a breach of section 1457 of the CCQ.

129. As a result of the breaches of the CCQ, the class members resident in Québec are entitled to moral and material damages pursuant to articles 1457 and 1463-1464 of the CCQ.

130. In addition, class members resident in Québec are entitled to punitive damages pursuant to article 49 of the Charter of Human Rights and Freedoms.

~~**Consumer Protection Claims**~~

131. ~~Class members are consumers within the meaning of the Applicable Consumer Protection Legislation because they entered into a consumer agreement with Innomar where Innomar agreed to provide goods or services for payment. In some instances, class members~~

paid directly for medical services that were not eligible for coverage under the applicable provincial publicly funded health care insurance plan. In other instances, Innomar supplied the services to the class member but the payment was made on behalf of the class member by the province in which the transaction occurred. Nevertheless, in the case where the payment was made by the province, class members were parties to the service agreements or were third party beneficiaries to them.

132. Innomar's failure to take reasonable measures to secure class members' personal information constitutes a deceptive practice under the Applicable Consumer Protection Legislation because Innomar's security measures did not meet the standards Innomar described in representations it set out in its privacy policies or which were required by PIPEDA, as detailed above.

133. Innomar's failure to notify customers that it was continuing to collect and store their personal information long after it was necessary is a misrepresentation by omission that constitutes a deceptive practice.

134. By making the false, misleading or deceptive representations about the state of its cyber-security and its ability the maintain the Class Members' privacy, Innomar engaged in deceptive practices, contrary to section 5 of the *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2 ("BPCPA") and contrary to parallel provisions of the Applicable Consumer Protection Legislation. Innomar is liable to the Class for the damages suffered as a result of the false, misleading and deceptive representations made by it.

135. It is not in the interests of justice to require that notice be given pursuant to section 18(15) of the Ontario *Consumer Protection Act*, and pursuant to parallel provisions of the Applicable Consumer Protection Legislation (where such notice is required), and therefore this condition should be waived.

136. As a result of the breaches of the Applicable Consumer Protection Legislation, class members have suffered damages for the false and misleading representations made to them by Innomar.

137. With respect to class members resident in Québec, Innomar is subject to the obligations of the *Consumer Protection Act*, CQLR c P-40.1, which prohibits persons who enter into agreements or conduct transactions with consumers from engaging in prohibited practices. Innomar's failure to take reasonable measures to secure class members' personal

~~information constitutes a prohibited practice because the representations that Innomar made to the class members in relation to its security measures were false and misleading, contrary to section 219.~~

138. ~~As a result of the breaches of the *Consumer Protection Act*, CQLR c P-40.1, class members resident in Québec have suffered damages for the false and misleading representations made to them by Innomar. In addition, class members resident in Québec are entitled to punitive damages pursuant to s. 272 of the *Consumer Protection Act*, CQLR c P-40.1.~~

~~Competition Act Claims~~

139. ~~Class members have a claim for damages under the Competition Act, R.S.C. 1985, c. C-34, s. 52 and 36, on the basis of the facts pleaded at paragraph 83 above. As set out above, Innomar knowingly or recklessly made materially false or misleading representations to the public regarding the state of their cyber-security. The representations were materially false or misleading for the same reasons pleaded at paragraphs 78-79 above.~~

140. ~~The representations caused Class Members to sustain damages by providing their personal information to the defendants. As a result of the representations the Class Members claim damages under s. 36(1)(a) for the breach of s 52.~~

DAMAGES

141. ~~As a consequence of the defendants' conduct and the unauthorized access of personal information and health information , the plaintiff and class members had their privacy deeply invaded and have suffered moral, general, non-pecuniary and compensatory damages, including but not limited to.~~ The plaintiff and class members had their privacy deeply invaded and have suffered damages including but not limited to:

a) Prolonged Mental distress;

b) Humiliation;

c) Anguish;

d) Stress;

e) Anxiety;

f) Violations of their right to informational privacy; and

g) Out-of-pocket expenses incurred to protect themselves from fraudulent activities, such as payments for additional credit monitoring.

142. In addition, the plaintiff and class members have suffered or will likely suffer further damage from identity theft and/or fraud in the event that their PHI and FI ~~personal and health information~~ was, and remains, available to the unauthorized third parties and may be used for criminal purposes. It is likely or, alternatively, there is a real and substantial chance that in the future the PHI and FI ~~personal and health information~~ may be released or sold on the internet causing further privacy violations or be used for criminal purposes such as to create fictitious bank accounts or engage in other forms identity theft and/or fraud, thereby causing the class members to suffer damages.

143. Finally, class members have suffered moral, general, non-pecuniary and compensatory damages for the violations of their privacy caused by both defendants and the hacker.

Negligence Acts

144. The plaintiff pleads and relies on the British Columbia Negligence Act [RSBC 1996] Chapter 333 section 4(2)(a); the Negligence Act, RSO 1990, c N.1, section 1; the Contributory Negligence Act, RSS 1978 c C-31, section 3(2); the Contributory Negligence Act, RSA 2000, c C-27, sections 1 and 2; the Contributory Negligence Act, RSNB 2011, c 131, sections 1 and3; the Tortfeasors and Contributory Negligence Act, CCSM c T90, sections 2 and 5; the Contributory Negligence Act, RSNS 1989, c 95, section 3; the Contributory Negligence Act, RSPEI 1988, c C-21, section 1; the Contributory Negligence Act, RSY 2022 c 42, section 1; the Contributory Negligence Act, RSNWT 1988, c C-18, sections 2 and 3; and the Contributory Negligence Act, RSNL 1990, c C-33, section 3 (collectively, the "Equivalent Negligence Legislation")

145. As a direct result of the defendants' breaches of the statutory privacy tort statutes as pleaded above, the hacker was able to unlawfully gain access to class members' PHI and FI.

~~personal and medical information resulting in a further privacy breach to the class.~~ The tort committed by the defendants by their breach of the privacy tort statutes combined with the intentional tort committed by the hacker ~~through its breach of~~ by unlawfully gaining access to the database and thereby breaching the privacy tort statutes caused class members to sustain indivisible compensatory, moral, general, non-pecuniary and pecuniary damages including distress, humiliation, anguish, reduced trust, feelings of lost privacy, and ongoing increased levels of stress as a result of the combined tortious conduct of the joint tortfeasors. The defendants and the hacker are therefore jointly and severally liable for all class member damages under the statutory torts pursuant to the Negligence Act of British Columbia and equivalent legislation as pleaded above at paragraph 144.

STATUTES

146. The plaintiff and class members plead and rely upon:

Civil Code of Québec, C.Q.L.R. c. C.C.Q.-1991

Class Proceedings Act, ~~1992~~, S.O. 1992, c. 6 [R.S.B.C. 1996], c. 50

Courts of Justice Act, R.S.O. 1980, c. 43

Personal Health Information Protection Act, 2004 S.O. 2004, c. 3

Personal Information Protection and Electronic Documents Act, SC 2000, c 5

Privacy Act, RSBC 1996, c 373

The Privacy Act, CCSM c Pl 25

The Privacy Act, RSS 1978, c P- 24

The Privacy Act, RSNL 1990, c P-22.

THE PLACE OF TRIAL

147. The plaintiff proposes that this action be tried at the City of Vancouver.

Date: October 30, 2024

Amended: April 14, 2025

Ted Charney

Signature of Theodore P. Charney
lawyer for plaintiff

Form 11 (Rule 4-5 (2))

ENDORSEMENT ON ORIGINATING PLEADING OR PETITION FOR SERVICE OUTSIDE BRITISH COLUMBIA

The plaintiff claims the right to serve this pleading/petition on the Defendants outside British Columbia on the ground that:

The circumstances in section 10 of the Court Jurisdiction and Proceedings Transfer Act are sections 10(e) because it concerns contractual obligations to a substantial extent were to be performed in British Columbia ~~and by its express terms, the contract is governed by the laws of British Columbia;~~ and 10 (h) concerns a business carried on in British Columbia

Plaintiff's address for service:	**CHARNEY LAWYERS PROFESSIONAL CORP.** 602 - 151 Bloor Street West Toronto, ON M5S 1S4
Fax number address for service (if any):	1-416-964-7416
E-mail address for service (if any):	tedc@charneylawyers.com
Place of trial:	Vancouver
The address of the registry is:	800 Smithe Street, Vancouver

Date: October 30, 2024

Ted Charney

Signature of Theodore P. Charney
lawyer for plaintiff

Rule 7-1 (1) of the Supreme Court Civil Rules states:

> (1) Unless all parties of record consent or the court otherwise orders, each party of record to an action must, within 35 days after the end of the pleading period,
>
> (a) prepare a list of documents in Form 22 that lists
>
> (i) all documents that are or have been in the party's possession or control and that could, if available, be used by any party at trial to prove or disprove a material fact, and
>
> (ii) all other documents to which the party intends to refer at trial, and
>
> (b) serve the list on all parties of record.

Appendix

[*The following information is provided for data collection purposes only and is of no legal effect.*]

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

Proposed class action regarding damages suffered as a result of a cyber security breach which occurred in early 2024~~3~~ wherein threat actors ~~a hacker~~ exfiltrated from the defendants the Personal Health Information and Financial Information ~~personal information~~ of clients of the defendant, Cencora Inc. and Innomar Strategies Inc. ~~MacKenzie Financial Corporation.~~

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

[*Check one box below for the case type that best describes this case.*]

A personal injury arising out of:

a motor vehicle accident

medical malpractice

X another cause

A dispute concerning:

contaminated sites

construction defects

real property (real estate)

personal property

the provision of goods or services or other general commercial matters

investment losses

the lending of money

an employment relationship

a will or other issues concerning the probate of an estate

X a matter not listed here

Part 3: THIS CLAIM INVOLVES:

[*Check all boxes below that apply to this case*]

X a class action

maritime law

aboriginal law

constitutional law

conflict of laws

none of the above

do not know

Part 4:

[*If an enactment is being relied on, specify. Do not list more than 3 enactments.*]

a) *Class Proceedings Act*, R.S.B.C. 1996, c. 50

b) *PIPEDA*, S.C. 2000 c. 5